






# V2X Tolling System for C-ITS Environments

Emanuel Vieira<sup>1</sup>, Tiago Dias<sup>2</sup>, João Almeida<sup>3</sup>, Ana V. Silva<sup>2</sup>, Joaquim Ferreira<sup>4</sup>  
and Lara Moura<sup>2</sup>

<sup>1</sup>*Instituto de Telecomunicações, Departamento de Eletrónica, Telecomunicações e Informática, Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal*

<sup>2</sup>*A-to-Be Mobility Technology S.A., Lagoas Park, Ed. 15, Piso 4, 2740-267 Porto Salvo, Portugal*

<sup>3</sup>*Instituto de Telecomunicações, Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal*

<sup>4</sup>*Instituto de Telecomunicações, Escola Superior de Tecnologia e Gestão de Águeda, Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal*

**Keywords:** V2X Tolling, Electronic Toll Collection, Vehicular Communications, Connected Vehicles, Cooperative Intelligent Transportation Systems.

**Abstract:** Electronic Toll Collection (ETC) has several decades of history worldwide. Vehicle-to-everything (V2X) communication technology is a more recent innovation but has been a central topic in the ITS community for more than a decade now. However, V2X technology adoption in vehicles has been limited and applications are mostly related to safety use cases. In this paper, V2X-based tolling applications are studied, as well as their feasibility, and how these applications could be enablers of a more massive V2X adoption in vehicles. V2X Tolling standards and solutions from SAE and ETSI are explored. A novel solution is presented, followed by a comparison with previous proposals and standards. Finally, preliminary results from the proposed system are presented and analyzed.


## 1 INTRODUCTION


Tolling is an industry with several decades of history worldwide. It is used mostly to finance infrastructure investment. The ease of use for customers provided through the employment of different types of wireless communications, together with visual recognition technology, has been the main driver for its modernization.


In 2012, the European Union had a 72 000 km toll road network with 60% covered by ETC at the time (Council of the European Union, 2017). Most of the ETC solutions were using microwave Dedicated Short Range Communication (DSRC) technology (Oh et al., 1999). Automatic Number Plate Recognition (ANPR) (Patel et al., 2013), and, more recently, satellite (GNSS) (Salós et al., 2013) and mobile communications (GSM) (Lee et al., 2004) based


solutions also emerged.


V2X communication technology has enabled communications between vehicles and with the infrastructure. It is a more recent innovation relative to tolling but it has been a central topic in the ITS community for more than a decade now. However, V2X technology adoption in vehicles has been limited and the usage is mostly linked with safety use cases. Current safety use cases may not be enough motivation for the public that is more used to getting live traffic information and routing through mobile applications in smartphones. V2X Tolling positions itself as a convenience use case, avoiding stops, cumbersome manual payment systems, or simply the need to purchase additional devices that operate on batteries that need to be replaced from time to time. With V2X, tolling may well be the right motivation for the public to see value in such convenience use cases and trigger the uptake of V2X in vehicles. ETC solutions have proved very successful in European markets (Council of the European Union, 2017), even though they require the acquisition of dedicated On-Board Units (OBUs) that typically need to be placed on the windshield and require periodic battery replacement. V2X

<sup>a</sup>  <https://orcid.org/0000-0001-9466-4649>

<sup>b</sup>  <https://orcid.org/0009-0009-1785-7119>

<sup>c</sup>  <https://orcid.org/0000-0001-6634-6213>

<sup>d</sup>  <https://orcid.org/0000-0003-0328-1787>

<sup>e</sup>  <https://orcid.org/0000-0002-7471-5135>

Tolling would provide the advantage of already coming in the vehicle and not requiring any battery replacement.

V2X Tolling can also take advantage of its security mechanisms to provide and ensure correct vehicle characteristics for the transactions, eliminating the need for vehicle classification on the infrastructure side. Similar mechanisms could be used for the vehicle to assess and report its passenger occupancy as part of High-Occupancy Tolling (HOT) scenarios.

Furthermore, the use of V2X communications could enable a more flexible tolling framework, with the implementation of virtual tolling plazas that can be dynamically moved inside the wireless range of Roadside Units' (RSUs) coverage areas according to the needs of road operators or city managers. Similarly, dynamic pricing could be easily implemented, by varying the cost of tolling payments for the same plaza throughout the day, e.g. based on road congestion levels or other time-varying metrics, and advertising this pricing information via nearby RSUs.

More recently, there has been a movement towards the adoption of V2X devices for Vulnerable Road Users (VRUs) (ETSI, 2020b), namely for those using lighter modes of transport such as bicycles. This could pave the way for even more widespread adoption of V2X fee collection or even V2X payments, with the added benefit of supporting a distance from the payment receiver devices that NFC is not capable of supporting.

In this paper, tolling applications using V2X communications and their feasibility are explored. An overview of the standardization efforts in the USA by SAE (SAE International, 2022), and in Europe by ETSI (ETSI, 2020a) is provided, complementing these with a newly proposed solution based on the ETSI ITS communication protocol stack for vehicular communications. The proposed system includes two distinct variants, one relying on TLS and TCP session establishment (TLS-V2XT) and another one based on the Geonetworking protocol and security framework (GN-V2XT).

The rest of the paper is divided as follows. Section 2 provides an overview of V2X Tolling standards and related work and implementations. Section 3 presents the proposed solution for V2X Tolling, its architecture and describes the implementation options taken in each protocol layer of the solution. In Section 4, this solution is compared and contextualized with standards and other implementations. Section 5 presents preliminary results of field trials using the proposed V2X Tolling solution. Finally, Section 6 concludes this paper by providing conclusions and an outlook of the next steps.

## 2 RELATED WORK

V2X Tolling has been identified as a feasible use case since the beginning of V2X communication systems development (Li et al., 2011).

In 2020, ETSI published a pre-standardization study on payment applications for Cooperative ITS (C-ITS) using Vehicle-to-Infrastructure (V2I) communications (ETSI, 2020a) based on the works of (Randriamasy et al., 2019a) and (Randriamasy et al., 2019b). This study presents different tolling and fee collection scenarios such as plaza systems, free flow tolling, and other payment applications such as parking, energy charging, ferries, and even drive-ins. It then proposes a proof-of-concept V2X Tolling solution that fits into the C-ITS stack and focuses on two main aspects: high-accuracy vehicle location using GNSS; and communication security. This is motivated by the intrinsic differences between the typical DSRC communications used for ETC and V2X communications. DSRC communications for ETC use a single device (antenna) for each lane, which is optimized to communicate with only a single vehicle on that lane at a time, while V2X has a much wider range of up to 1 km. This means that, with DSRC, the lane the vehicle is passing through is directly identified by the receiving antenna and there is less chance for the communication between the vehicle device and the DSRC antenna to be interfered with. With V2X, the location of the vehicle can be anywhere within the large communication radius covered by the V2X device, and anyone within that radius can interfere with those communications.

This proof-of-concept was implemented over DSRC ITS-G5 V2X communications using IPv6, TCP, and TLS to establish secure channels between RSUs and OBUs. While the secure TLS channel is used for the fee collection transaction itself, prior to its establishment, RSUs broadcast open Service Announcement Essential Messages (SAEM) (ETSI, 2019) which OBUs use to get information about the RSU tolling functionality and to initiate the secure channel.

This solution was trialed in France by the motorway operator SANEF on more than one hundred passages in Taissy and Senlis toll lanes, with 100% accuracy in detecting the correct toll lane of passage and 100% success in charging the transaction using V2X.

(ETSI, 2020a) positions V2X Tolling as a Value-Added Service (VAS) within the V2X ecosystem, as a standard solution adaptable to other standards such as IEEE 1609.11 (IEEE, 2011) and identifies it as having the potential to provide a much more cost-effective solution for ETC, with much simpler maintenance

requirements than existing ETC infrastructures and with the ability to expand into numerous other services such as parking or drive-in purchases.

In parallel, in the United States, SAE published in 2022 the J3217 standard for V2X-Based Fee Collection (SAE International, 2022). It is a complete standard for V2X fee collection, implemented over the WAVE protocol using either DSRC or C-V2X (PC5 interface) communications. J3217 focuses on V2X Tolling use cases by dividing them into three main scenarios:

- Road segment pricing – covering current main road toll booth payment points, Multi-Lane Free Flow (MLFF) / Open Road Tolling (ORT), and High-Occupancy Tolling (HOT) scenarios.
- Closed network pricing – covering entry and exit toll systems.
- Object pricing – covering the use of specific objects like tunnels, ferries, passes, or parks.

The standard moves from a high-level definition of the entities involved in V2X Tolling and the relations between them to the definition of the actual communications protocol using ASN.1 notation to define three main message types:

- Toll Advertisement Message (TAM) – is transmitted by RSUs to announce tolling point data including toll zone geometry and fees.
- Toll Usage Message (TUM) – is transmitted by the OBU in each vehicle to which a toll fee applies. It includes the necessary data for the Tolling system to charge the road user.
- Toll Usage Message acknowledgment (TUMack) – is transmitted by the RSU directed at a specific vehicle / OBU to confirm the TUM has been correctly received.

The protocol is designed to guarantee privacy and security in TUM messages through the use of encryption, and has a general concern for privacy, through the use of a rolling certificate mechanism for the OBU encryption and signing of the messages.

The fee model supports different types of tariffs:

- Fixed fee by vehicle class/type, weight, or the number of axles.
- Distance-based fees according to origin/destination also supporting different vehicle classes/types, weights, or the number of axles.
- Time-based fees (like the ones used in car parks).
- Vehicle occupancy-based variations for the fees to support High-Occupancy Tolling.

IEEE 1609.2 (IEEE, 2016) certificates are used for signing TAM and TUMack messages, and for the signature and encryption of TUM messages, using 256-bit or 384-bit Elliptic Curve Cryptography (ECC). While ECDSA is used for signing, ECIES is used for encryption purposes.

This standard also explores possible enforcement techniques in a short appendix.

The last V2X Tolling scenario proposed in (SAE International, 2022), referred to as "object pricing", can be generalized from tolling to fee collection to include in-vehicle payments for on-street and off-street parking, drive-through restaurants, pharmacies, fuelling, carwash, shopping pickup, and several other types of in-vehicle provided services that can be paid using V2X. This can easily become a mass convenience service if the supporting infrastructure costs are low and the vehicle uptake is high.

Recently, some works have introduced the use of more emergent forms of cryptography to V2X-based ETC systems like Distributed Ledger Technologies (DLT), including blockchains, and Zero-Knowledge Proofs (ZKPs) to enhance the security and privacy of ETC systems. Assuring the position accuracy of the vehicle is important to ensure that only the ones passing through specified zones are charged. (Didouh et al., 2020) expands on this issue by proposing a localization system based on distance estimation through Received Signal Strength Indication (RSSI) values analysis, and the recording of related Proof-of-Location (PoL) data in a blockchain, where it is further processed. (McEntyre and Kihei, 2022) proposes a ZKP-based system to enhance user privacy by preventing exploitation of vehicle location through the use of continuous challenges issued by the RSU to nearby OBUs that do not provide location data for ETC purposes. Focusing on authentication and client privacy, (Bartolomeu et al., 2020) uses the concepts of Self-Sovereign Identity (SSI) and cryptocurrency payments to provide mutual authentication between OBU and RSU using ZKP, and then actually pay the value of the toll due using a DLT, so that both processes (authentication and payment) take place within the tolling zone.

While these latter works can greatly enhance user privacy by employing popular emergent technologies and techniques, the proposed solution focuses on the OBU-RSU communications protocol using established and faster cryptography schemes, similar to what is being proposed within standardization bodies.

### 3 V2X TOLLING SYSTEM

In this paper, a new V2X Tolling system is proposed. It is based on (ETSI, 2020a) but with custom Facilities-layer Tolling messages, named Tolling Payment Messages (TPM), handled and generated by a new Facilities sub-service named Tolling Payment (TP). This TP service executes the tolling transactions and transmits them over a secure channel based on ITS-G5 V2X communications. It also employs SAEMs for RSUs to announce the tolling service and provide the necessary information for in-vehicle OBUs to establish secure channels with the RSUs.

One of the protocol variants of this solution is closer to (ETSI, 2020a) and uses TLS as a secure channel for the exchange of TPM. This protocol variant is named TLS-V2XT.

Establishing a TLS channel over ITS-G5 involves two additional network layers with TCP on top of IPv6 (see Figure 1), which can add a significant amount of overhead traffic, in some scenarios, to establish and maintain the channel (e.g., TLS negotiation, TCP acknowledge messages, etc.). Taking this into account and the fact that ITS-G5 already has a powerful encryption feature usable within the GeoNetworking protocol, a different approach is proposed to V2X Tolling altogether. In this second approach, the same SAEM message is used but the TLS channel is not established, being the TPM messages directly sent over BTP and GeoNetworking with GeoNetworking’s native encryption and signing features and implementing a retransmission mechanism for messages that get no reply. This other protocol variant is called GN-V2XT.

While TLS-V2XT was implemented essentially to assess the feasibility of (ETSI, 2020a) and study its viability for free flow scenarios, GN-V2XT was designed as a novel approach, closer to the options taken in other ITS-G5 protocols such as CAM, DENM or IVIM.

Figure 1 shows the protocol stack for SAEM, GN-V2XT, and TLS-V2XT in a single image. SAEM are Facilities layer messages, using BTP and GeoNetworking for the Transport and Networking layer, respectively, and ETSI TS 103 097 in the Security part, specifically for signing the messages at the networking level. GN-V2XT uses the same stack options as SAEM but also uses ETSI TS 103 097 Security for encryption of TPM Facilities layer messages. TLS-V2XT uses TLS for Security, TCP for Transport, and IPv6 for Networking layers with the same TPM Facilities layer messages. All messages in both these protocols use the ITS-G5 LLC for the Access layer but could be adapted to employ C-V2X technology.

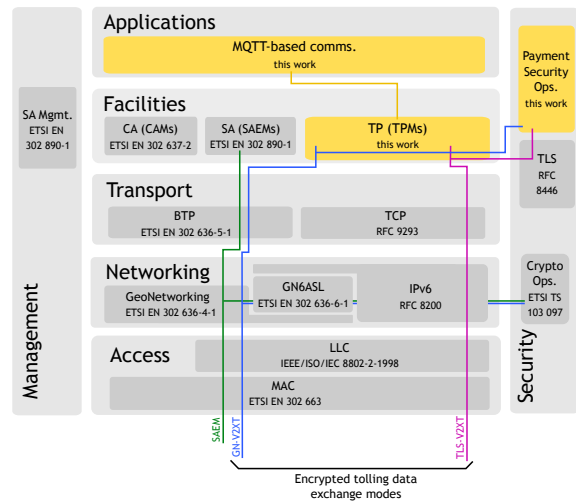


Figure 1: Protocol stack comparison between the two proposed V2X Tolling schemes.

Both solutions (TLS-V2XT and GN-V2XT) are examined in the following subsections for each protocol layer, identifying the differences between the two protocols as well as their similarities.

#### 3.1 Facilities

The Facilities layer handles and generates the messages related to the toll service advertisement (SAEMs) and the messages related to the toll transaction (TPMs), which are common to both TLS-V2XT and GN-V2XT.

##### 3.1.1 Service Announcement

In order to make OBUs aware of nearby tolls, SAEMs are continuously broadcasted by RSUs at a rate of 1 Hz, advertising an ETC service (ITS-AID = 1, as defined in ISO 17419). The radio channel used is ETSI ITS-G5 SCH ( 5.9 GHz).

Tolling zones are included in SAEMs, encoded in a new structure named Tolling Payment Info (TPI). A TPI is composed by the ID of the tolling zone, the tolling zone itself as a sequence of coordinates defining a polygonal area, the traffic flowing angle, and the toll type, which can be either entry, exit, or single.

RSUs in the vicinity of the tolling zones broadcast the TPIs in their SAEM.

##### 3.1.2 Tolling Payment Message (TPM)

A new ITS message type named Tolling Payment Message (TPM) is introduced to enable V2X Tolling services. It is based on a request-reply mechanism, being initiated by the OBU which issues a TPM request when it enters a tolling zone, followed by a

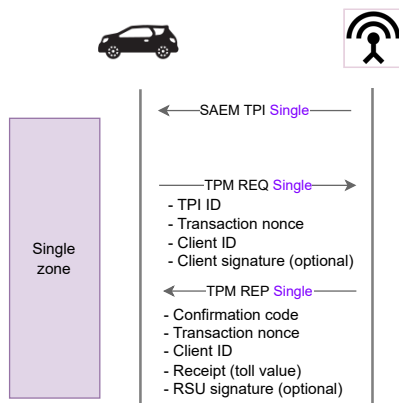


Figure 2: Single tolling system protocol.

TPM reply issued by the RSU. The protocol is implemented at the ETSI ITS Facilities layer. All TPM messages received and transmitted by the RSU and OBUs are published in an MQTT broker, by a module running in the Application layer, for mobile app and cloud integration purposes. TPMs support both single toll (ORT or plazas) and closed tolling systems.

In a single tolling system (see Figure 2), when the OBU detects it is inside a tolling zone, it broadcasts a single encrypted TPM request that can only be decrypted by the local RSU. This message includes the TPI identification number, a nonce that identifies that specific request, the client identification number associated with the tolling company, and an optional client signature, which may or may not be mandatory depending on the communication mechanism used, as described in the next subsection.

The RSU replies with a single encrypted TPM reply that can only be decrypted by the OBU. This message includes a confirmation code, depending on whether the RSU accepted the request or not, the nonce of the request, the client identification number, a receipt with the monetary value of the toll due, and an optional RSU signature.

In a closed toll system (see Figure 3), upon entering the motorway, if the OBU detects that it is inside a toll entry zone, it broadcasts an encrypted TPM entry request that can only be decrypted by the local RSU. This message includes the TPI identification number, a nonce that identifies this specific request, the client identification number associated with the tolling company, and optionally, a client signature.

The RSU replies with an encrypted TPM entry reply only decryptable by the OBU. This message includes a confirmation code, depending on whether the RSU accepted the request or not, the nonce of the request, the client identification number, and a mandatory RSU signature. This TPM must be signed as it will be used by the OBU as proof of entry.

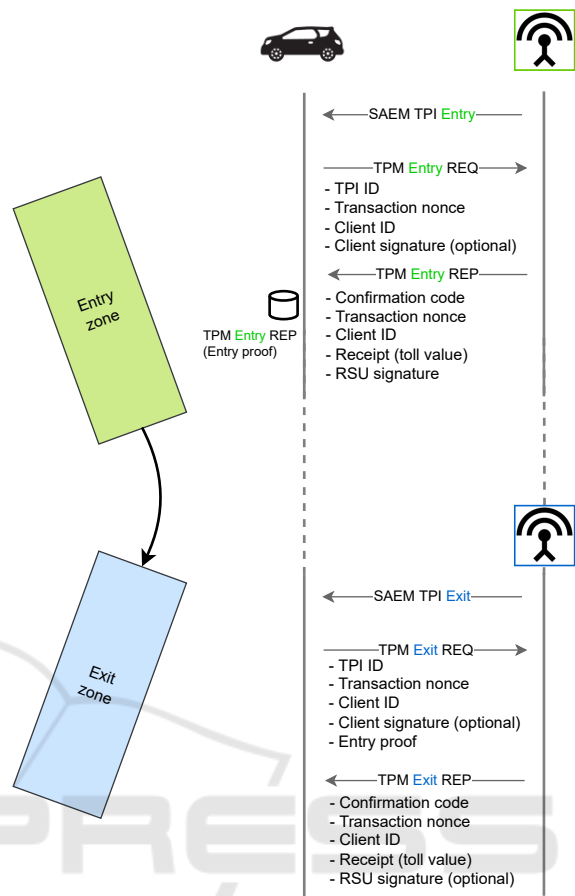


Figure 3: Closed tolling system protocol.

Upon exiting the motorway, if the OBU detected it is inside a toll exit zone, it broadcasts an encrypted TPM exit request that can only be decrypted by the local RSU. This message includes the TPI identification number, a nonce that identifies this specific request, the client identification number associated with the tolling company, the entry proof and, lastly, an optional client signature.

The RSU replies with an encrypted TPM exit reply, only decryptable by the OBU. This message includes a confirmation code associated with the RSU having accepted or not the request, the nonce of the request, the client identification number, a receipt with the monetary value of the toll due value, and an optional RSU signature.

The entry proof acts as a way for the RSU to verify in which place the OBU has entered the motorway. All TPMs contains a timestamp which can also be analyzed for entry/exit analysis to avoid malicious behavior. In case the entry proof is not provided by the OBU at the exit, the toll value due is to be defined in accordance with the tolling company's policy.

## 3.2 Security

To safeguard client privacy, communication between the OBU and the RSU must be encrypted. Authentication is also required to ensure that the RSU belongs to a trusted tolling company and that the OBU belongs to an authorized client.

At the security level, the two proposed schemes (TLS-V2XT and GN-V2XT) follow different approaches with the same goal of providing secure TPM exchange.

### 3.2.1 TLS (TLS-V2XT)

In TLS-V2XT, two different sets of certificates are used. In the ETSI ITS protocol stack, vehicles and RSUs must have by default a set of temporary certificates (set A) named Authorizations Tickets (ATs), which act as pseudonyms. ATs provide authentication in the vehicular network, privacy, and unlinkability through their short-lived timespan and rotatory mechanism. These certificates are used for signing SAEMs. A tolling company should, in principle, not be able to link an AT with a user's identity, therefore it must be able to authenticate users and RSUs using a PKI of its own. This is achieved by using another set of certificates, issued by the tolling company or tolling agency. This other set of certificates (set B) is based on X.509 and is used to set up the TLS channel. TLS provides encryption and authentication based on the tolling company's PKI to secure the TPM exchange. Both the client (OBU) and RSU are mutually authenticated. The TLS channel is implemented using OpenSSL.

### 3.2.2 GeoNetworking Security (GN-V2XT)

In GN-V2XT, as in TLS-V2XT, GeoNetworking provides authentication on the local vehicular network by signing SAEM messages (ECDSA 256-bit) using ATs (set A). For encryption and user authentication of TPM messages, GN-V2XT employs a second set of certificates (set C), inspired by the ETSI ITS PKI and based on the ETSI TS 103 097 standard, as a substitute for set B. Set C is also produced by the PKI of the tolling company or agency. The ECIES encryption scheme, implemented using OpenSSL, is used in GN-V2XT to secure the TPM exchange.

## 3.3 Transport

The Transport Layer protocol used in each V2X tolling system approach is different.

### 3.3.1 TCP (TLS-V2XT)

In TLS-V2XT, TCP provides a reliable communication channel. It is implemented using an adapted version of an open-source TCP implementation. The adapted version provides additional functionality as well as support for IPv6 instead of IPv4.

To protect against packet loss, in TLS-V2XT the TCP retransmission mechanism ensures the arrival of timed-out packets when the transmitter does not receive an acknowledgment from the receiver. In this implementation, the TCP timeout is set to 200 milliseconds.

### 3.3.2 BTP (TLS-V2XT & GN-V2XT)

The Basic Transport Protocol (BTP) is used in the Transport layer, to encapsulate SAEMs in both schemes and to encapsulate TPMs in the GN-V2XT approach. Since BTP does not have any retransmission features, in GN-V2XT a retransmission mechanism of the TPM messages was implemented. The OBU retransmits the TPM request after a timeout is reached and until it receives the TPM reply from the RSU. In this implementation, the timeout is set to 400 milliseconds. This retransmission mechanism is implemented in the Facilities layer by the TP service, and not in the Transport layer.

## 3.4 Network

The Network Layer protocol employed is distinct for each V2X tolling system approach.

### 3.4.1 IPv6 (TLS-V2XT)

In TLS-V2XT, IPv6 provides addressing. A raw implementation is used, capable of encapsulating and decapsulating IPv6 packets with simple addressing capabilities. Packet hopping is currently not implemented.

### 3.4.2 GeoNetworking (GN-V2XT)

GN-V2XT uses GeoNetworking for the Networking layer, as it is done for SAEMs. The encryption and decryption of secure TPM packets happen in this layer through requests to the Security service. Both the TPM and the BTP header are encrypted.

## 4 SOLUTION COMPARISON

A comparison between the V2X Tolling solutions TLS - ETSI TR (ETSI, 2020a), SAE (SAE Interna-

Table 1: Overall comparison among the different V2X Tolling solutions.

Feature	TLS-ETSI TR	TLS-V2XT (this work)	SAE	GN-V2XT (this work)
Announcement	SAEM	SAEM	TAM	SAEM
Communications Complexity (# messages)	13	7	3	3
Authentication	TLS w/ ECC	TLS w/ ECC	ECDSA	ECDSA
ETC application certificates	ETSI TS 103 097-based	X509-based	IEEE WAVE-based	ETSI TS 103 097-based
Encryption	TLS	TLS	ECIES	ECIES
Retransmission	TCP	TCP	On timeout after TUM transmission	On timeout after TPM request transmission

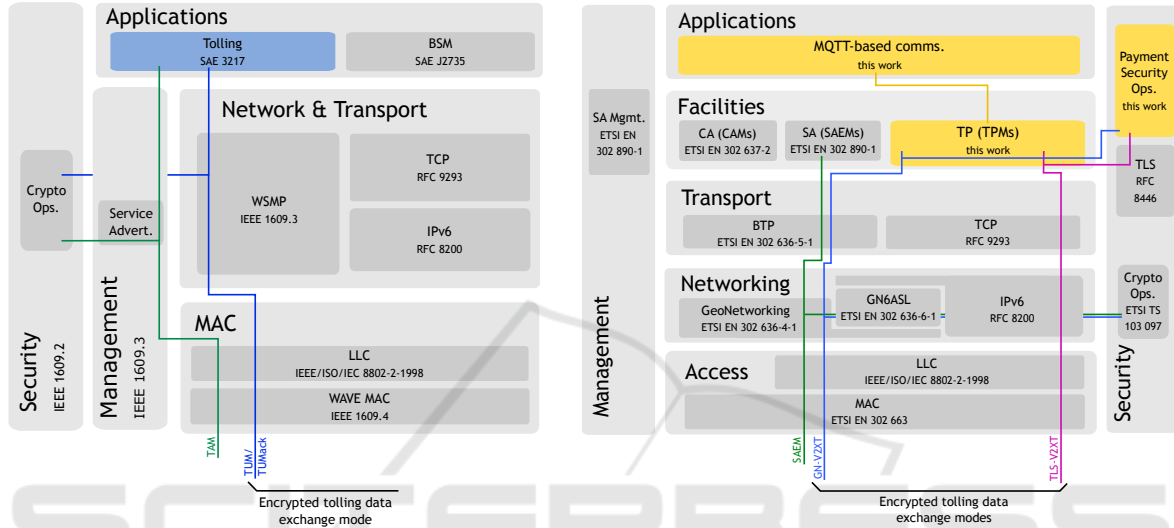


Figure 4: Protocol stacks and supporting standards for SAE V2X Tolling vs. GN-V2XT + TLS-V2XT.

tional, 2022), and the two newly proposed variant schemes is given in Table 1. The protocol stacks used are also detailed in Figure 4. All designs follow the same approach to communication logic: nearby RSUs continuously broadcast the tolling service via SAEMs or TAMs, and vehicles initiate P2P encrypted communications with the advertising RSU when entering a tolling zone. A small exception is a design in the TLS-ETSI TR, where the RSU, after mutual authentication, and when the vehicle enters the paying zone (detected through trajectory analysis from Cooperative Awareness Messages - CAMs - emitted by the OBU), initiates the toll transaction by issuing a request for the client information.

Due to the multi-step message exchange in TLS-ETSI TR, first for the SAEM announcement message (1 message), then the establishment of the TCP (2 messages) and TLS (2 messages) sessions, i.e., the handshakes, then for the authentication of the vehicle for eligibility for the ETC service (2 messages), and finally for the actual exchange of the payer information (5 messages and 1 final confirmation message), this solution has the highest communication complexity, totalling 13 distinct messages. The proposed TLS-V2XT implementation reduces

the communication complexity as only the TPM request and TPM reply are exchanged after the TCP and TLS handshakes. Using ECIES, both in SAE and in the GN-V2XT design, only two messages are exchanged, the TUM and TUMack, or the TPM request and TPM reply, respectively. Communication complexity is not related to the performance of the communication scheme, as TLS has lower computational requirements than ECIES due to lighter cryptography. However, in scenarios with significant packet loss, communication performance can be severely degraded in designs with higher communication complexity due to the higher probability of the need for (more) packet retransmissions.

Authentication is provided by TLS using elliptic curve cryptography (ECC) in TLS-ETSI TR and TLS-V2XT or by ECDSA in the other implementations, typically using 256 or 384-bit curves. Separate sets of certificates are used by the ITS-Station (ITS-S) for authentication in the vehicular network during normal operation and for authentication with the tolling system. These sets are different in order to separate the tolling service provider information from the user's vehicular data, thereby increasing user privacy.

User privacy is also enhanced by the encryption

used in the communication protocol, as personally identifiable information must be communicated between the vehicle and the RSU to perform the toll transaction. The general logic for establishing a private and secure channel between ITS-Ss is similar in both TLS and ECIES schemes: using the public keys (asymmetric cryptography, slower) present in the ITS-S certificates, the ITS-S derives an encryption key (symmetric cryptography, faster) that is used to encrypt the communication channel.

Given the possibility of packet loss, messages must be retransmitted after a timeout. In the case of the TLS designs, TCP safeguards packet delivery by retransmitting packets if respective acknowledgments are not received before a timeout. In SAE and on the GN-V2XT design, the OBU retransmits the TUM and TPM request, respectively, if the corresponding responses, the TUMack and TPM reply, are not received before a timeout.

Although the SAE V2X Tolling standard rests on top of IEEE WAVE protocol stack and both GN-V2XT and TLS-V2XT (as well as the originating TLS-ETSI TR) rely on a different one (ETSI ITS-G5), there are more architectural similarities between SAE V2X Tolling and GN-V2XT than between GN-V2XT and TLS-V2XT. In both SAE V2X Tolling and GN-V2XT, authentication, and encryption are handled in the Network layer (using ECIES for encryption and ECDSA for authentication in both cases) and retransmission is the responsibility of the Application or Facilities layer.

As for the tolling protocol itself, TLS-ETSI TR uses a more complex protocol than SAE V2X Tolling or the newly proposed schemes. TLS-ETSI TR includes intermediate phases (vehicle tracking, etc.) other than the transaction itself. It would be desirable to avoid the need for such phases and still be able to use the tracking information from vehicles in the vicinity of the tolling areas to distinguish between passages in different lanes. This could be achieved by having the RSU or the central system tracking vehicles in the vicinity of the tolls using CAM or Basic Safety Messages (BSM) and, once a transaction is initiated, fetch this information for a use or discard it if it's not used within a specified time interval.

It is important to note that the SAE V2X Tolling standard is prepared for more payment scenarios than the implementations proposed in this work, including even features for HOT or other scenarios such as an object or time-based fee collection.

Given the provided comparison, GN-V2XT and SAE V2X Tolling are more lightweight than TLS-V2XT and the original protocol used in (ETSI, 2020a), in respect to network usage, while providing

a higher degree of security. Meanwhile, both GN-V2XT and SAE V2X Tolling have a higher processing demand from RSUs for the encryption algorithm than TLS used in TLS-V2XT and the original protocol used in (ETSI, 2020a). The main differences between GN-V2XT and SAE V2X Tolling are the usage of different V2X stacks (ITS-G5 and WAVE respectively) and the fact that the authorization scheme in GN-V2XT is detached from the vehicular security system running at lower levels of the communication stack, which does not happen in SAE V2X Tolling. This means that GN-V2XT is able to offer greater control over authorized customers to tolling authorities, agencies and enterprises. This decoupling of the vehicular security system and payment protocols could potentially enhance the security and privacy of the tolling system by reducing the likelihood of unauthorized access and protecting sensitive user information.

## 5 PRELIMINARY RESULTS

The proposed solution was first validated in laboratory tests, followed by three sets of road tests in Portugal, two in the Aveiro region, and one in Lisbon. Both GN-V2XT and TLS-V2XT variants were tested in the laboratory and the first Aveiro region trials, where some preliminary results were obtained. Regarding these first Aveiro road tests, Figure 5 depicts the tolling zone and RSU locations. The OBU and RSU are both composed of a PC Engines APU3D4 featuring an AMD GX-412TC 4-core CPU @ 1.4 GHz with 4 GB RAM and a Qualcomm Atheros AR928X Wi-Fi module adapted for ITS-G5. The OBU and RSU used in the tests were the only ITS-G5 transmitting stations in the vicinity, surrounded by mild traffic characterized in its majority by legacy (non-connected) vehicles. The RSU was installed at a high point, decreasing the probability of packet loss due to vehicles acting as obstacles.

The results of three runs are provided in Table 2, two for GN-V2XT (the average is provided) and one for TLS-V2XT. During each run, the OBU passed through the open system first and then through the closed system. The results are respective only to the open system. The open system tests were successful in this first trial, but the closed system tests failed because the entry toll zone was set too far away from the RSU that should be covering it, so there was no adequate ITS-G5 coverage on the exit Toll. Only the entry toll was adequately covered. This resulted in the OBU being unable to initiate communication with the RSU that should cover the exit toll. Follow-



up tests with the closed system scenario in Lisbon were successfully conducted, however, those results are not presented in this work since TLS-V2XT was not tested and the hardware used in those trials was significantly different in computational power, hindering any fair comparison.

Table 2 presents the obtained results for both implementations (GN-V2XT and TLS-V2XT), using an OBU and an RSU in a single tolling system scenario for the first road trial. The delays presented are measured from the time the OBU detects it is inside a tolling zone up until the instant it receives and finishes analyzing the TPM reply.

The results show the feasibility of the employed communication mechanisms and the proposed tolling system based on TPM messages. The measured delays are all below 200 ms, which is sufficient for a non-safety vehicular service such as tolling.

The proposed GN-V2XT variant is on par with the TLS-V2XT scheme in terms of communication latency.

However, the TLS option lacks some security features related to authentication during both the TCP and TLS handshakes, i.e., handshake messages are not authenticated, potentially enabling some types of denial-of-service attacks. This scheme also has a higher communication complexity as 7 messages are exchanged (1 for SAEM announcement, 2 for the TCP handshake, 2 for the TLS handshake, and 2 for the secured TPMs).

In the GN-V2XT scheme, which uses heavier cryptography (ECIES), only 1 SAEM announcement message and 2 TPM messages are exchanged (the secured pair of TPM request and reply), which can be beneficial in higher packet loss scenarios. The use of ECIES is also more in line with the ETSI ITS standards which are employed in other V2X applications (i.e., certificate requests to CAs). Ultimately, ECIES is much more widely deployed in commercial ETSI ITS OBUs/RSUs than TLS is.

More systematic testing with hundreds of repetitions in both schemes is required for a more thorough analysis.



Figure 5: Single tolling scenario used for the first road trial.

Table 2: V2X Tolling delay in a single zone scenario.

		Transaction delay (ms)
[t]	GN-V2XT	94.991
	TLS-V2XT	79.197

## 6 CONCLUSIONS & FUTURE WORK

This paper has shown that V2X Tolling is not only possible but also can be the enabler for mass market adoption of V2X technology. Meanwhile, ETC DSRC technology still shows interoperability issues. V2X could position itself as a fully interoperable tolling solution to overcome these barriers and make V2X Tolling as universal as credit card payments are today. V2X Tolling could also have the added benefit of being able to provide proof of vehicle classification and other data elements such as passenger occupancy.

This work analysed the US Standard from SAE (SAE International, 2022) (for IEEE WAVE and C-V2X) and several working prototypes (using ETSI ITS-G5) documented in (ETSI, 2020a) and in this paper. All of these have adopted strong security mechanisms and use retransmission mechanisms to ensure message delivery over unreliable vehicular communications channels.

In this paper, two main V2X Tolling approaches using ITS-G5 were presented: TLS-V2XT and GN-V2XT. TLS-V2XT is based on TLS-ETSI TR (ETSI, 2020a) and uses a TLS channel setup over ITS-G5 using TCP and IPv6. GN-V2XT uses a custom retransmission mechanism over the existing ITS-G5 stack with BTP for Transport and GeoNetworking for Networking and Security. Both use TPM, a custom set of Facilities-layer messages, for the tolling transactions. GN-V2XT shares with SAE (SAE International, 2022) the options for Security protocols (ECDSA and ECIES), the custom retransmission of messages, and the reduced number of messages exchanged in a tolling transaction (only three packets are transmitted when there is no packet loss).

Initial trials have been carried out with the proposed schemes, but these are not yet sufficient to benchmark the two protocols and validate the success rate on large volumes of traffic. Setting up benchmarking and larger-scale trials are the next milestones. For now, it was possible to show the transaction times are below 100 milliseconds and how a RSU with a slower CPU will take longer to process GN-V2XT than TLS-V2XT due to the higher CPU demand of the encryption used in GN-V2XT.

After extended tests of both GN-V2X and TLS-V2XT over ITS-G5, it is also planned to implement

and test both over C-V2X and NR-V2X, in order to benchmark the results against ITS-G5 technology.

With a solid standard in the US, the next natural steps for V2X Tolling would be to develop and adopt a standard in Europe, to progress with larger field trials, and to gather momentum with automotive manufacturers and infrastructure operators, paving way for a wider adoption.

## REFERENCES

- Bartolomeu, P. C., Vieira, E., and Ferreira, J. (2020). Pay as you go: A generic crypto tolling architecture. *IEEE Access*, 8:196212–196222.
- Council of the European Union (2017). Proposal for a directive of the European parliament and of the council on the interoperability of electronic road toll systems and facilitating cross-border exchange of information on the failure to pay road fees in the union. Procedure 2017/0128/COD.
- Didouh, A., Lopez, A. B., El Hillali, Y., Rivenq, A., and Al Faruque, M. A. (2020). Eve, you shall not get access! a cyber-physical blockchain architecture for electronic toll collection security. In *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, pages 1–7. IEEE.
- ETSI (2019). Intelligent Transport Systems (ITS); Facilities layer function; Part 1: Services Announcement (SA) specification. Technical Report EN 302 890-1 V1.2.1, European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France.
- ETSI (2020a). Intelligent Transport Systems (ITS); Pre-Standardization Study on payment applications in Cooperative ITS using V2I communication. Technical Report TR 103 579 V1.1.1, European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France.
- ETSI (2020b). Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 3: Specification of VRU awareness basic service; Release 2. Technical Report TS 103 300-3 V2.1.1, European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France.
- IEEE (2011). IEEE Standard for Wireless Access in Vehicular Environments (WAVE)– Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS). Technical Report 1609.11-2010, IEEE, Piscataway, New Jersey, United States.
- IEEE (2016). IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages. Technical Report 1609.2-2016, IEEE, Piscataway, New Jersey, United States.
- Lee, W.-H., Jeng, B.-S., Tseng, S.-S., and Wang, C.-H. (2004). Electronic toll collection based on vehicle-positioning system techniques. In *IEEE International Conference on Networking, Sensing and Control, 2004*, volume 1, pages 643–648. IEEE.
- Li, M.-W., Wu, T.-H., Lin, W.-Y., Lan, K.-C., Chou, C.-M., and Hsu, C.-H. (2011). On the feasibility of using 802.11 p for communication of electronic toll collection systems. *International Scholarly Research Notices*, 2011.
- McEntyre, J. and Kihei, B. (2022). Zero-knowledge proof for enabling privacy preserving electronic toll collection with vehicle-to-everything communications. In *2022 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–6. IEEE.
- Oh, H., Yae, C., Ahn, D., and Cho, H. (1999). 5.8 ghz dsr packet communication system for its services. In *Gateway to 21st Century Communications Village. VTC 1999-Fall. IEEE VTS 50th Vehicular Technology Conference (Cat. No. 99CH36324)*, volume 4, pages 2223–2227. IEEE.
- Patel, C., Shah, D., and Patel, A. (2013). Automatic number plate recognition system (anpr): A survey. *International Journal of Computer Applications*, 69(9).
- Randriamasy, M., Cabani, A., Chafouk, H., and Fremont, G. (2019a). Formally validated of novel tolling service with the its-g5. *IEEE Access*, 7:41133–41144.
- Randriamasy, M., Cabani, A., Chafouk, H., and Fremont, G. (2019b). Geolocation process to perform the electronic toll collection using the its-g5 technology. *IEEE Transactions on Vehicular Technology*, 68(9):8570–8582.
- SAE International (2022). V2X-Based Fee Collection; Surface Vehicle Standard. Technical Report J3217-202206, SAE International, Warrendale, Pennsylvania, United States.
- Salós, D., Martineau, A., Macabiau, C., Bonhoure, B., and Kubrak, D. (2013). Receiver autonomous integrity monitoring of gnss signals for electronic toll collection. *IEEE transactions on intelligent transportation systems*, 15(1):94–103.